

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) Data sequence randomization-encryption system that making use of freely selectable control block with plaintext sequence generates substantially at random sequence, comprising:

a first input means for receiving a plaintext sequence(X),

a second input means for receiving a control block (Kp),

an assembly means of blocks of length N (301) which assemble said plaintext sequence (X) in a plurality of plaintext blocks (XI),

a control block dividing means (1001) which divide said control block (Kp) into a control initial block of length G (R) and a control initial block of length 2N (Z),

a transformer block generating means (1002) which with said control initial block of length G (R) and a plurality corresponding randomized-encrypted text block (YI) generate a plurality of transformer blocks (WTI),

a generating means of encryption control subblocks (202) which with said control initial block of length 2N (Z) generate a plurality of encryption control subblocks (Z_1 - Z_{52}),

a grouping means (603) which group corresponding said plaintext block (XI) and corresponding said transformer block (WTI), generating a grouped interblock (VI),

a staged encrypting-decrypting means (204) which encrypt said grouped interblock (VI) with said plurality of encryption control subblocks (Z_1 - Z_{s2}), generating said randomized-encrypted text block (YI),

an output supplying means (302) which supply plurality said randomized-encrypted text block (YI) making up a randomized-encrypted text sequence (\underline{Yp}),
whereby said randomized-encrypted text sequence (\underline{Yp}) corresponds to said plaintext sequence (\underline{X}) received by said first input means,

wherein said transformer block generating means (1002) generate said transformer block (WTI; WTJ) implementing a function H (said control initial block of length G (R), said randomized-encrypted text block (YI; YJ)).

wherein said grouping means (603) include an exclusive-OR operation,

wherein said transformer block generating means (1002) implement said function H (said control initial block of length G (R), said randomized-encrypted text block (YI; YJ)) as

for first said transformer block (WTI; WTJ) includes said control initial block of length G (R),

for nth said transformer block (WTI; WTJ) is equal to nth minus one said randomized-encrypted text block (YI; YJ) XOR nth minus one said transformer block (WTI; WTJ).

2. (Canceled)

3. (Currently Amended) Data sequence randomization-encryption system that making use of control initial block of length $2N$ freely selectable with plaintext sequence generates substantially at random sequence, comprising:

a first input means for receiving a plaintext sequence (X),

a second input means for receiving a control initial block of length $2N$ (Z),

an assembly means of blocks of length N (301) which assemble said plaintext sequence (X) in a plurality of plaintext blocks (XI),

a transformer block generating means (1002) which with a control initial block of length G (R) and a plurality corresponding randomized-encrypted text blocks (YI) generate a plurality of transformer blocks (WTI),

a generating means of encryption control subblocks (202) which with said control initial block of length $2N$ (Z) generate a plurality of encryption control subblocks (Z_1 - Z_{s2}),

a grouping means (603) which group corresponding said plaintext block (XI) and corresponding said transformer block (WTI), generating a grouped interblock (VI),

a staged encrypting-decrypting means (204) which encrypt said grouped interblock (VI) with said plurality of encryption control subblocks (Z_1 - Z_{s2}), generating said randomized-encrypted text block (YI),

an output supplying means (302) which supply plurality said randomized-encrypted text block (YI) making up a randomized-encrypted text sequence (Yp), whereby said randomized-encrypted text sequence (Yp) corresponds to said plaintext sequence (X) received by said first input

means,

wherein said transformer block generating means (1002) generate said transformer block (WTI;WTJ) implementing a function H (said control initial block of length G (R), said randomized-encrypted text block (YI;YJ)),

wherein said grouping means (603) include an exclusive-OR operation,

wherein said transformer block generating means (1002) implement said function H (said control initial block of length G (R), said randomized-encrypted text block (YI;YJ)) as

for first said transformer block (WTI;WTJ) includes said control initial block of length G (R),

for nth said transformer block (WTI;WTJ) is equal to nth minus one said randomized-encrypted text block (YI;YJ) XOR nth minus one said transformer block (WTI;WTJ).

4. (Canceled)

5. (Canceled)

6. (Canceled)

7. (Currently Amended) The system of claim 6 1 wherein said transformer block generating means (1002) implement said function H (said control initial block of length G (R), said randomized-encrypted text block (YI;YJ)) for nth said transformer block (WTI; WTJ) equal to nth block of length N generated by a function E_n (said control initial block of length G (R)) XOR nth minus one said randomized-encrypted text block (YI;YJ).

8. (Original) The system of claim 7 wherein said transformer block generating means (1002) implement said function E_n (said control initial block of length $G(R)$) as $E_n(R_i) = (E_{n-1}(R_i) \text{ oper } B) \bmod 2^{Q_i}$, wherein said Q_i less than or equal to 64 said R_i of length said Q_i is subblock of said control initial block of length $G(R)$, said oper arithmetic operation selected from the group consisting of addition and subtraction and shift, said B a value, said mod module operation.

9. (Original) The system of claim 8 wherein said control initial block of length $2N(Z)$ made up preferably of 128 bits and said control initial block of length $G(R)$ made of preferably of 64 bits.

10. (Original) The system of claim 7 wherein said transformer block generating means (1002) implement said function E_n (said control initial block of length $G(R)$) including a random number generator.

11. (Original) The system of claim 10 wherein said control initial block of length $2N(Z)$ made up preferably of 128 bits and said control initial block of length $G(R)$ made up preferably of seed length of said random number generator.

12. (Original) The system of claim 7 wherein said transformer block generating means (1002) implement said function E_n (said control initial block of length $G(R)$) including a hash function.

13. (Original) The system of claim 12 wherein said control initial block of length $2N(Z)$ made up preferably of 128 bits and said control initial block of length $G(R)$ made up preferably of zero or more bits.

14. (Canceled)

15. (Currently Amended) The system of claim ~~14~~ 1 wherein said control initial block of length $2N(Z)$ made up preferably of 128 bits and said control initial block of length $G(R)$ made up preferably of 64 bits.

16. (Currently Amended) The system of claim ~~6~~ 1 wherein said transformer block generating means (1002) implement said function H (said control initial block of length $G(R)$), said randomized-encrypted text block $(YI; YJ)$ as

for first said transformer block $(WTI; WTJ)$ is said control initial block of length $G(R)$,

for n th said transformer block $(WTI; WTJ)$ is n th minus one said randomized-encrypted text block $(YI; YJ)$.

17. (Original) The system of claim 16 wherein said control initial block of length $2N$ (Z) made up preferably of 128 bits and said control initial block of length G (R) made up preferably of 64 bits.

18. (Currently Amended) The system of claim ~~6~~ 1 wherein said transformer block generating means (1002) implement said function H (said control initial block of length G (R), said randomized-encrypted text block (YI;YJ)) for n th said transformer block (WTI;WTJ) equal to n th block of length N generated by a function E_n (n th minus one said randomized-encrypted text block (YI;YJ)) XOR said control initial block of length G (R).

19. (Original) The system of claim 18 wherein said transformer block generating means (1002) implement said function E_n (n th minus one said randomized-encrypted text block (YI;YJ)) as $E_n(Y_i) = (E_{n-1}(Y_i) \text{ oper } B) \bmod 2^{Q_i}$, wherein said Q_i less than or equal to 64, said Y_i of length said Q_i is subblock of said n th minus one said randomized-encrypted text block (YI;YJ), said oper arithmetic operation selected from the group consisting of addition and subtraction and shift, said B a value, said mod module operation.

20. (Original) The system of claim 19 wherein said control initial block of length $2N$ (Z) made up preferably of 128 bits and said control initial block of length G (R) made up preferably of 64 bits.

21. (Original) The system of claim 18 wherein said transformer block generating means (1002) implement said function E_n (nth minus one said randomized-encrypted text block (YI;YJ)) including a hash function.

22. (Original) The system of claim 21 wherein said control initial block of length $2N$ (Z) made up preferably of 128 bits and said control initial block of length G (R) made up preferably of zero or more bits.

23. (Canceled)

24. (Canceled)

25. (Canceled)

26. (Canceled)

27. (Canceled)

28. (Canceled)

29. (Canceled)

30. (Canceled)

31. (Canceled)

32. (Canceled)

33. (Canceled)

34. (Canceled)

35. (Canceled)

36. (Canceled)

37. (Canceled)

38. (Canceled)

39. (Canceled)

40. (Canceled)

41. (New) The system of claim 3 wherein said control initial block of length $2N$ (Z) made up preferably of 128 bits and said control initial block of length G (R) made up preferably of 64 bits.

42. (New) Data sequence randomization-encryption system that making use of freely selectable control block with plaintext sequence generates substantially at random sequence, comprising:

a first input means for receiving a plaintext sequence(X),

a second input means for receiving a control block (K_p),

an assembly means of blocks of length N (301) which assemble said plaintext sequence (X) in a plurality of plaintext blocks (XI),

a control block dividing means (1001) which divide said control block (K_p) into a control initial block of length G (R) and a control initial block of length $2N$ (Z),

a transformer block generating means (1002) which with said control initial block of length

G (R) and a plurality corresponding randomized-encrypted text block (YI) generate a plurality of transformer blocks (WTI),

a generating means of encryption control subblocks (202) which with said control initial block of length $2N$ (Z) generate a plurality of encryption control subblocks (Z_1 - Z_{s2}),

a grouping means (603) which group corresponding said plaintext block (XI) and corresponding said transformer block (WTI), generating a grouped interblock (VI),

a staged encrypting-decrypting means (204) which encrypt said grouped interblock (VI) with said plurality of encryption control subblocks (Z_1 - Z_{s2}), generating said randomized-encrypted text block (YI),

an output supplying means (302) which supply plurality said randomized-encrypted text block (YI) making up a randomized-encrypted text sequence (Yp),

whereby said randomized-encrypted text sequence (Yp) corresponds to said plaintext sequence (X) received by said first input means,

wherein said transformer block generating means (1002) generate said transformer block (WTI; WTJ) implementing a function H (said control initial block of length G (R), said randomized-encrypted text block (YI; YJ)),

wherein said grouping means (603) include an exclusive-OR operation,

wherein said transformer block generating means (1002) implement said function H (said control initial block of length G (R), said randomized-encrypted text block (YI; YJ)) as

for first said transformer block (WTI; WTJ) is said control initial block of length G (R),

for nth said transformer block (WTI; WTJ) is nth minus one said randomized-encrypted text block (YI; YJ).

43. (New) The system of claim 42 wherein said control initial block of length $2N$ (Z) made up preferably of 128 bits and said control initial block of length G (R) made up preferably of 64 bits.

44. (New) Data sequence randomization-encryption system that making use of control initial block of length $2N$ freely selectable with plaintext sequence generates substantially at random sequence, comprising:

a first input means for receiving a plaintext sequence (X),

a second input means for receiving a control initial block of length $2N$ (Z),

an assembly means of blocks of length N (301) which assemble said plaintext sequence (X) in a plurality of plaintext blocks (XI),

a transformer block generating means (1002) which with a control initial block of length G (R) and a plurality corresponding randomized-encrypted text blocks (YI) generate a plurality of transformer blocks (WTI),

a generating means of encryption control subblocks (202) which with said control initial block of length $2N$ (Z) generate a plurality of encryption control subblocks (Z_1 - Z_{s2}),

a grouping means (603) which group corresponding said plaintext block (XI) and

corresponding said transformer block (WTI), generating a grouped interblock (VI),

a staged encrypting-decrypting means (204) which encrypt said grouped interblock (VI) with said plurality of encryption control subblocks (Z_1 - Z_{s2}), generating said randomized-encrypted text block (YI),

an output supplying means (302) which supply plurality said randomized-encrypted text block (YI) making up a randomized-encrypted text sequence (\underline{Yp}), whereby said randomized-encrypted text sequence (\underline{Yp}) corresponds to said plaintext sequence (\underline{X}) received by said first input means,

wherein said transformer block generating means (1002) generate said transformer block (WTI;WTJ) implementing a function H (said control initial block of length G (R), said randomized-encrypted text block (YI;YJ)),

wherein said grouping means (603) include an exclusive-OR operation,

wherein said transformer block generating means (1002) implement said function H (said control initial block of length G (R), said randomized-encrypted text block (YI;YJ)) as

for first said transformer block (WTI;WTJ) is said control initial block of length G (R),

for nth said transformer block (WTI;WTJ) is nth minus one said randomized-encrypted text block (YI;YJ).

45. (New) The system of claim 44 wherein said control initial block of length $2N$ (Z) made up preferably of 128 bits and said control initial block of length G (R) made up preferably of 64 bits.